

SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1373

# **Analiza i usporedba sigurnosnih mehanizama u Internetu stvari**

Filip Ptiček

Zagreb, svibanj 2021.

## **DIPLOMSKI ZADATAK br. 1373**

Pristupnik: **Filip Ptiček (0036491837)**  
Studij: Informacijska i komunikacijska tehnologija  
Profil: Telekomunikacije i informatika  
Mentor: izv. prof. dr. sc. Marin Vuković

Zadatak: **Analiza i usporedba sigurnosnih mehanizama u Internetu stvari**

### Opis zadatka:

Posljednjih godina razvoj bežičnih pristupnih mreža te energetski efikasnih ugradbenih računala ima za posljedicu pojavu malih uređaja koji nude mogućnosti kontrole, mjerenja i praćenja okoline. Jedan od izazova Interneta stvari je sigurnost i privatnost korisnika te njihovih podataka. Taj izazov je posebno naglašen zbog heterogenosti uređaja i protokola za komunikaciju potrebnih kod implementacije sustava. Vaš je zadatak istražiti i usporediti postojeće tehnologije i protokole za komunikaciju te zaštitu podataka u okolini Interneta stvari. Na temelju istraživanja potrebno je osmisliti i implementirati rješenje na kojem ćete analizirati protokole u smislu osiguravanja osnovnih sigurnosnih zahtjeva.

Rok za predaju rada: 28. lipnja 2021.



# SADRŽAJ

<b>1. Uvod</b>	<b>1</b>
<b>2. Internet stvari</b>	<b>2</b>
2.1. Definicija . . . . .	2
2.2. Model IoT sustava . . . . .	2
2.3. Čimbenici u sustavu . . . . .	2
2.4. Programske platforme . . . . .	2
2.5. Otvorena pitanja . . . . .	2
2.5.1. Sigurnost . . . . .	2
2.5.2. Privatnost . . . . .	2
2.5.3. Skalabilnost . . . . .	3
2.5.4. Decentraliziranost . . . . .	3
2.6. Primjene . . . . .	3
2.6.1. Područja primjene . . . . .	3
2.6.2. Zahtjevi sustava s obzirom na primjenu . . . . .	3
2.7. Trendovi . . . . .	3
<b>3. Sigurnosni zahtjevi u Internetu stvari</b>	<b>4</b>
3.1. OWASP Top 10 . . . . .	4
3.1.1. Slabe, pogodljive ili tvrdo kodirane lozinke . . . . .	4
3.1.2. Nesigurne mrežne usluge . . . . .	5
3.1.3. Nesigurna sučelja ekosustava . . . . .	6
3.1.4. Nedostatak mehanizama za sigurnosna ažuriranja . . . . .	7
3.1.5. Upotreba nesigurnih ili zastarijelih komponenti . . . . .	8
3.1.6. Nedovoljna zaštita privatnosti . . . . .	8
3.1.7. Nesigurni prijenos i pohrana podataka . . . . .	10
3.1.8. Nedostatak mogućnosti upravljanja uređajima . . . . .	11
3.1.9. Nesigurne zadane postavke . . . . .	11

3.1.10. Nedostatak fizičke sigurnosti . . . . .	11
3.2. Primjeri sigurnosnih napada i propusta . . . . .	11
<b>4. Analiza i usporedba protokola</b>	<b>12</b>
4.1. IoT stack . . . . .	12
4.2. Fizički sloj . . . . .	12
4.2.1. Analiza uređaja . . . . .	12
4.2.1.1. Senzori s komunikacijskim modulom . . . . .	12
4.2.1.2. Pristupni uređaji . . . . .	12
4.2.2. Usporedba sigurnosnih mehanizama i primjena . . . . .	12
4.3. Sloj podatkovne poveznice . . . . .	12
4.3.1. Analiza tehnologije protokola . . . . .	13
4.3.1.1. WiFi . . . . .	13
4.3.1.2. BLE . . . . .	13
4.3.1.3. RFID\NFC . . . . .	13
4.3.1.4. ZigBee . . . . .	13
4.3.1.5. LTE . . . . .	13
4.3.1.6. SigFox . . . . .	13
4.3.1.7. LoRaWan . . . . .	13
4.3.2. Usporedba sigurnosnih mehanizama i primjena . . . . .	13
4.4. Mrežni sloj . . . . .	13
4.4.1. Analiza protokola . . . . .	14
4.4.1.1. IPv4 . . . . .	14
4.4.1.2. IPv6 . . . . .	14
4.4.2. Usporedba sigurnosnih mehanizama i primjena . . . . .	14
4.5. Transportni sloj . . . . .	14
4.5.1. Usporedba primjena protokola . . . . .	14
4.6. Aplikacijski sloj . . . . .	14
4.6.1. Analiza protokola . . . . .	14
4.6.1.1. HTTP/S . . . . .	14
4.6.1.2. COAP . . . . .	14
4.6.1.3. MQTT . . . . .	15
4.6.2. Usporedba sigurnosnih mehanizama i primjena . . . . .	15
<b>5. Sustav za praćenje tjelesne temperature</b>	<b>16</b>
5.1. Arhitektura sustava . . . . .	16

5.2. Korišteni razvojni alati i uređaji . . . . .	16
5.3. Opis rada sustava . . . . .	16
5.4. Sigurnosna analiza sustava . . . . .	16
<b>6. Zaključak</b>	<b>17</b>
<b>Literatura</b>	<b>18</b>
<b>Popis slika</b>	<b>19</b>
<b>Popis tablica</b>	<b>20</b>

# **1. Uvod**

Uvod u rad

## **2. Internet stvari**

### **2.1. Definicija**

a

### **2.2. Model IoT sustava**

a

### **2.3. Čimbenici u sustavu**

a

### **2.4. Programske platforme**

a

### **2.5. Otvorena pitanja**

a

#### **2.5.1. Sigurnost**

a

#### **2.5.2. Privatnost**

a



### **2.5.3. Skalabilnost**

a

### **2.5.4. Decentraliziranost**

a

## **2.6. Primjene**

a

### **2.6.1. Područja primjene**

a

### **2.6.2. Zahtjevi sustava s obzirom na primjenu**

a

## **2.7. Trendovi**

a

## 3. Sigurnosni zahtjevi u Internetu stvari

### 3.1. OWASP Top 10

The Open Web Application Security Project® (OWASP) je neprofitna organizacija čiji je cilj napredak i poboljšanje računalne sigurnosti informacijskih sustava. OWASP kroz svoje projekte otvorenog koda vođenih putem razvojne zajednice radi na poboljšanju sigurnosti Interneta.

*OWASP Internet of Things Project* je projekt osmišljen kako bi pomogao proizvođačima, programerima i potrošačima bolji uvid i razumijevanje u sigurnosne probleme vezane uz Internet stvari. Na taj način korisnici u bilo kojem dijelu razvojnog procesa mogu donositi bolje odluke kod razvoja, postavljanja i pristupanja tehnologijama Interneta stvari.[3] 2018. godine izlazi *OWASP IoT Top 10* lista koja reprezentira deset najčešćih ranjivosti Internet stvari sustava. Svih deset sigurnosnih ranjivosti su navedeni u nastavku uz opis sigurnosnih zahtjeva koji bi trebali spriječiti te ranjivosti i sigurnosne propuste.

#### 3.1.1. Slabe, pogodljive ili tvrdo kodirane lozinke

Prvi navedeni sigurnosni problemi kod Internet stvari sustava su vezni uz lozinke. Kako bi se uređaju moglo pristupiti i naknadno ga konfigurirati, uređaji dolaze s korisničkim računima koji služe korisnicima kako bi ih mogli upariti sa željenim sustavim ili kako bi proizvođač mogao upravljati uređajem u slučaju pomoći korisnicima ili ažuriranja uređaja. Za pristup tom korisničkom računu uređaja je potrebna lozinka koju krajnji korisnik kod prve upotrebe treba postaviti. Navike korisnika su većinom da iskoriste njima dobro poznatu lozinku koju koriste i za svoje druge korisničke račune. Ako napadač dobije pristup jednoj njihovoj lozinci ima i pristup ostalim računima. Na taj način se pristup korištenim uređajima koji imaju isto korisničko ime ili e-mail

adresu i lozinku uvelike olakšava. Korisnici imaju i naviku koristiti slabe lozinke koje su vrlo česte i jako lako pamtljive. Tako su neke od najčešće korištenih lozinka jednostavni nizovi numeričkih znakova ili nizovi znakova na tipkovnici poput: 123456, 123456789, qwerty, ili sam engleski prijevod lozinke (engl. *password*).[6]. Napadi na lozinke se provode putem takozvanih *brute force* napada. Kako je procesna snaga današnjih računala dosegla vrlo visoke brzine računanja, tako se jednostavne i kratke lozinke mogu pogoditi u vrlo kratkom vremenu.

Ovakvi propusti ne zaobilaze ni proizvođače samih sustava i uređaja. Kod proizvodnje proizvođači na uređaje postavljaju iste lozinke za sve uređaje kako bi kod testiranja ispravnosti lakše pristupili istima. Jedan od najboljih pokazatelja takvog pristupa su usmjerivači/modemi telekom operatera za pristup Internetu koji imaju postavljenu istu zadanu lozinku i korisničko ime poput "admin" ili "user" koju krajnji korisnici uređaja nikada ne promjene. Problem se također pojavljuje i u tvrdo kodiranim (engl. *hard coded*) lozinkama. Proizvođači postave takve lozinke na uređaje kako bi se uređaji mogli nesmetano povezati s vanjskim servisima, kako bi se proizvođači povezali na uređaj zbog otklanjanja pogrešaka ili kao način za vanjsko upravljanje uređaja. Ako napadač ima fizički pristup uređaju on može skenirati memoriju i pomoću raznih alata pronaći lozinku spremljenu na samom uređaju. A kako proizvođači najvjerojatnije koriste istu lozinku za sve iste modele uređaja, napadač ima lak način za pristup i ostalim istim uređajima.

Kako bi se spriječila ova vrsta ranjivosti neki od sigurnosnih zahtjeva koji bi se trebali pratiti su sljedeći. Korisnici bi kod prve upotrebe uređaja trebali promijeniti zadanu lozinku koristeći duge, kompleksne i jedinstvene nizove znakova. Najjednostavniji način postići te zahtjeve je korištenjem upravitelja lozinkama. Oni daju mogućnost generiranja lozinke uz mogućnost spremanja istih bez potrebe da korisnik mora pamtiti sve jedinstvene i duge lozinke. Što se tiče zahtjeva sa strane proizvođača, oni bi trebali razriješiti bolje načine upravljanja uređajima kako bi se izbjeglo korištenje istih ili čak tvrdo kodiranih lozinka za pristup uređaju ili vanjskim servisima. Također bi proizvođači trebali upozoriti korisnika kod uspostave uređaja da promijeni zadanu lozinku.

### **3.1.2. Nesigurne mrežne usluge**

Internet stvari uređaji koriste razne mrežne usluge kako bi mogli komunicirati s vanjskim servisima. Kako je moguće pristupiti tim uređajima putem Interneta potrebno je pravilno osigurati sigurnost tih mrežnih usluga koje se izvršavaju. Neautoriziran

pristup preko usluga iskorištavajući zadane lozinke, otvorene mrežne priključke te nepravilno podešeni vatrozidi dozvoljavaju napadaču da dobije pristup uređajima i poslužiteljima. Takvi napadi dozvoljavaju izvršavanje malicioznog koda, iskorištavanje uređaja za botnet, krađu podataka ili onesposobljavanje sustava.

Neki od sigurnosnih mjera koje se mogu poduzeti za osiguravanje mrežnih usluga su:

- korištenje zasebne lokalne mreže za sve pametne uređaje,
- spajati uređaje na isključivo sigurne mreže,
- instaliranje regularnih softverskih ažuriranja,
- isključivanje svih usluga koje pružaju vanjski pristup uređaju,
- isključivanje nepotrebnih mrežnih priključaka i usluga,
- isključivo korištenje protokola koji koriste enkripciju.

### **3.1.3. Nesigurna sučelja ekosustava**

Nesigurna web sučelja, pozadinski API-jevi, servisi u oblaku i mobilna sučelja, koja dozvoljavaju komunikaciju i interakciju s uređajem, čine sveukupni ekosustav Internet stvari. Kompromitacija bilo kojeg dijela sustava može uzrokovati i kompromitaciju cijelokupnog sustava. Ranjivost kod načina autorizacije i autentifikacije između uređaja i poslužitelja ili korisnika mobilnih i web aplikacija i poslužitelja su jedan od vektora napada na sustav. Također nedostatak ili korištenje slabe enkripcije kod komunikacije može uzrokovati da napadač presretne i iskoristi sakupljene informacije za napad. Nedostatak pravilnog filtriranja ulazno/izlaznih podataka može dovesti do napada poput SQL injekcije. Još jedan projekt OWASP organizacije je *OWASP Top 10 Web Application Security Risks* koji nudi popis najčešćih ranjivosti za web i mobilne aplikacije. Nesigurna sučelja ekosustava imaju direktnu poveznicu s tim ranjivostima koje su:

- injekcije (SQL, NoSQL, OS, LDAP),
- neispravna autentifikacija,
- izlaganje osjetljivih podataka,
- XML External Entities (XXE) napadi,
- neispravna autorizacijska kontrola,
- pogrešna konfiguracija servisa,
- Cross-Site Scripting (XSS),

- nesigurna deserijalizacija podataka,
- korištenje biblioteka i komponenta s poznatim sigurnosnim ranjivostima,
- nedovoljno korištenje logova i praćenja sustava.[2]

Pravilno podešavanje autorizacije i autentifikacije korisnika, ali i uređaja je najvažniji način osiguravanja raznih sučelja ekosustava. Filtriranje ulaznih i izlaznih podataka spriječava napade injekcijom, pravilno podešavanje poslužitelja da koriste pravilne enkripcijske načine komunikacije dozvoljavaju privatnu i sigurnu komunikaciju. Kroz cijeli ekosustav je potrebno i uspostava logiranja i praćenja sustava kako bi se na vrijeme otkrili nepravilna ponašanja unutar samog sustava.

### **3.1.4. Nedostatak mehanizama za sigurnosna ažuriranja**

Kroz vrijeme, za programska rješenja koja se trenutno koriste na uređaju će se pronaći ranjivosti. Kako bi se na vrijeme i jednostavnim putem mogli spriječiti napadi koji iskoristavaju te ranjivosti potrebna su nam softverska ažuriranja, kao i ažuriranja samog ugrađenog programa (engl. *firmware*) uređaja. Ako ne postoji način kojim dovodimo takva sigurnosna ažuriranja na uređaj postoji rizik za kompromitacijom uređaja. Također ako su i implementirani načini sigurnosnih ažuriranja, potrebno je pridodati pažnju na način te implementacije ažuriranja. Ako se ne provjeravaju digitalni potpisi izvora ažuriranja, moguće je na uređaj poslati maliciozno ažuriranje koje će kompromitirati uređaj. Potrebno je i koristiti sigurne načine prijenosa tih ažuriranja poput enkripcije upotrebljavanog komunikacijskog kanala.

Trenutnim trendom brzog razvoja novih uređaja, proizvođači često ne daju dovoljno dugi period sigurnosnih ažuriranja. Tako će se desiti da proizvod nakon manje od dvije godine prestane dobivati ažuriranja te će pasti odluka na korisnika o tome hoće li kupiti novi uređaj ili riskirati kompromitaciju istog. Najbolji pokazatelj toga su pametni telefoni od kojih većina tijekom svog perioda upotrebe dobije samo nekoliko sigurnosnih ažuriranja prije nego bude deprecirana od strane proizvođača.

Kako bi se uređaji zaštili od budućih napada zbog novootkrivenih sigurnosnih propusta potrebno je pružati korisnicima uređaja nuditi dugotrajna i česta sigurnosna ažuriranja. Prijenos ažuriranja je neophodno prenositi putem sigurnih komunikacijskih kanal koji su enkriptirani. Ažuriranjima koja su dostigla na uređaj je potrebno validirati izvor, provjeriti odgovara li digitalni potpis izvoru od kojeg bi trebalo stići ažuriranje. Također je potrebno i validirati samo ažuriranje kako bi se izbjeglo moguće umetanje malicioznog koda.

### 3.1.5. Upotreba nesigurnih ili zastarijelih komponenti

Nadovezano na nedostatak mehanizama za sigurnosno ažuriranje, peta po redu od sigurnosnih propusta je upotreba nesigurnih ili zastarijelih komponenti. Mnogi sustavi Internet stvari kao dio svojeg programskog rješenja sadrže otvoreni kod koji održava zajednica koja nije direktno povezana s proizvođačem. Kada se otkrije ranjivost na nekom od korištenih otvorenih rješenja proizvođač ili čeka na sigurnosnu zakrpu, ili u najboljem slučaju će sam riješiti sigurnosni propust te ga javno objaviti kako bi doprineo razvoju otvorenog rješenja. Nakon što sigurnosna zakrpa bude razvijena potrebno je ažurirati sve uređaje ili dijelove sustava koji su ugroženi od tog sigurnosnog propust.

Ako govorimo o Internetu stvari u proizvođačkoj industriji, takozvanoj Industrij 4.0, upotreba zastarijele programske podrške, koja je potrebna zbog jako specifičnih uređaja za proizvodnju, čija zadnja verzija zna datirati i više od deset godina nije rijetka. Uvođenjem takvih uređaja u sustave Interneta stvari također utječe na sigurnost i integritet cjelokupnog sustava te ugrožavanje jednog uređaja može dovesti do napada na cijelog lanca opskrbe. Kod upotrebe gotovih proizvoda poput senzora, videokamera ili pametne rasvijete te integracijom istih u postojeći sustav također treba obratiti pozornost na dostupnost sigurnosnih ažuriranja te stanje uređaja poput je li proizvođač još uvijek nudi sigurnosnu podršku.

Kod planiranja razvoja Internet stvari sustava potrebno je uzeti u obzir trenutno, a i buduće stanje razvojne i sigurnosne podrške vanjske programske potpore i komponenti sustava. Najbolji način za spriječavanje sigurnosnih propusta je korištenje vlastito razvijene programske potpore ili korištenje dobro podržanih vanjskih biblioteka otvorenog koda s jakom i aktivnom razvojnom zajednicom. Uporeba zastarijelih uređaja bez sigurnosne podrške proizvođača ili potporom koja uskoro dotiže krajnji period (engl. *end of life*) je potrebno izbjegavati. Nakon puštanja sustava u produkciju nadziranje i praćenje vijesti vezanih uz sigurnosne propuste upotrebljenih komponenti i programske podrške je važno kako bi se na vrijeme moglo spriječiti kompromitacija sustava. Sve ovo nije moguće ako bilo koji dio ustava nema implementirane mehanizme za sigurnosna ažuriranja. Ako neka od komponenti dostigne svoj krajnjio period ažuriranja potrebno je tu komponentu ukloniti i zamijeniti ju drugom čija sigurnosna ažuriranja još uvijek su podržana.

### 3.1.6. Nedovoljna zaštita privatnosti

Uloga Interneta stvari je djelom prikupljanje različitih podataka i mjerenja. Neki od tih podataka su osobne prirode za korisnika poput: medicinskih podataka ili zvukovnih

i video zapisa. Kompromitacija takvih privatnih podataka može negativno utjecati na sigurnost korisnika. Prostor na kojem se privatnost korisnika može narušiti je od samog uređaja koji prikuplja podatke, do komunikacijskih kanala preko kojih se podaci šalju do samih krajnjih servisa koji primaju i obrađuju te podatke, a zatim ih spremaju u baze podataka na poslužiteljima. Nedovoljna zaštita privatnosti je zapravo rezultat svih ostalih nabrojanih sigurnosnih ranjivosti nabrojanih u ovom odjeljku.

Za očuvanje privatnosti korisnika i načine obrade podataka korisnika u Europskoj uniji postoji uredba donešena od strane Europske unije pod nazivom *Opća uredba o zaštiti podataka (GDPR) (EU) 2016/679* [1]. Cilj uredbe je omogućiti građanima Europske unije veću kontrolu i uvid u podatke koji se prikupljaju. Na taj način građani mogu tražiti brisanje svojih podataka i povećava se odgovornost pravnih osoba koje te podatke prikupljaju. Odgovornost se postiže mogućim nametnutim sankcijama, ako se utvrdi povreda podataka građana. Prikupljanje podataka je moguće uz izrazitu privolu građana korisnika čime se zabranjuje bilo kakvo prikupljanje podataka bez pristanka.

Enkripcija komunikacijskih kanala nekada ne osigurava i privatnost korisnika. Kako bi pametni uređaji mogli komunicirati s krajnjim poslužiteljima, koji mogu mijenjati svoju odredišnu adresu, koriste se domenska imena. Za razlučivanje tih adresa u brojanje IP adrese koristi se protokol DNS (engl. *Domain Name System*). Kada uređaji rade DNS upite u sadržaju upita se prikazuje i domena upita u nekriptiranom formatu. Na taj način napadač može iz konteksta upita zaključiti koji uređaji proizvođača se nalaze u mreži korisnika. Za neke uređaje je moguće zaključiti i sam tip, a ne samo proizvođač. U sljedećoj tablici možemo vidjeti uređaje i DNS upite koje proizvode:

Uređaj	DNS upiti
Nest Security Camera	nexus.dropcam.com
	oculus519-vir.dropcam.com
	pool.ntp.org
Amazon Echo	ash2-accesspoint-a92.ap.spotify.com
	audio-ec.spotify.com
	device-metrics-us.amazon.com
	ntp.amazon.com
	pindorama.amazon.com
	softwareupdates.amazon.com

**Tablica 3.1:** Primjer DNS upita napravljenih od strane uređaja [4]

Još jedan način na koji se može zaključiti o trenutnoj aktivnosti korisnika u vlastitoj

mreži je i broj paketa koji se šalje u danom trenutku van mreže i njihova periodičnost. Ako se radi o uređaju koji ima mogućnosti virtualnog asistenta moguće je imati uvid u to kada je korisnik imao interakciju s uređajem. Također kod uređaja koji prate spavanje korisnika se broj razmijenjenih paketa drastično poveća kada korisnik spava.[4]

Kako najbolje očuvati privatnost korisnika je pitanje s kojim još uvijek mnogi proizvođači imaju problema. To se očituje u ostalim navedenim sigurnosnim propustima u ovom odjeljku. Zakonskim regulativama postiže se veća svijest o bitnosti zaštite podataka te se samim time proizvođači tjeraju na bolje prakse za očuvanjem podataka. Neki od osnovnih načina zaštite korisničkih podataka su:

- enkripcija podataka u svakom aspektu sustava,
- prikupljanje samo nužnih podataka,
- anonimiziranje korisnika,
- bolja kontrola i uvid u podatke za korisnike.

### **3.1.7. Nesigurni prijenos i pohrana podataka**

Podaci koji nisu kriptirani moguće je vrlo lako iščitati. Kriptografijom se postiže sigurnost i privatnost podataka. Kako bi se to postiglo podatke je potrebno kriptirati u svakom koraku njihova nastajanja, prijenosa, obrade i spremanja. Korištenje samih kriptografskih algoritama ne rezultira uvijek i zaštitom podataka. Neki kriptografski algoritmi koriste ključeve nedovoljne dužine i kao takve je potrebno malo vremena da se dešifriraju. Najveći sigurnosni propusti u nedavnoj povijesti povezani su direktno s nedovoljnim kriptografskim algoritmima ili općenitim nedostatkom šifriranja čime su ugroženi osobni podaci i lozinke korisnika.[5] Pozornost se treba posvetiti i kontroli pristupa podacima kako neautorizirani korisnici ne bi mogli pristupiti nedozvoljenim podacima.

Osnovni sigurnosni zahtjevi koji bi se trebali osigurati su:

- šifriranje podataka,
- pravilno korištenje PKI-a (engl. *public key infrastructure*),
- kontrola pristupa podacima,
- korištenje sigurnih protokola za prijenos podataka,
- provjera korištenih kriptografskih algoritama za ranjivosti,
- korištenje dugih kriptografskih ključeva.



### **3.1.8. Nedostatak mogućnosti upravljanja uređajima**

a

### **3.1.9. Nesigurne zadane postavke**

a

### **3.1.10. Nedostatak fizičke sigurnosti**

a

## **3.2. Primjeri sigurnosnih napada i propusta**

a

## **4. Analiza i usporedba protokola**

### **4.1. IoT stack**

Iot stack

### **4.2. Fizički sloj**

Senzori

#### **4.2.1. Analiza uređaja**

Uređaji

##### **4.2.1.1. Senzori s komunikacijskim modulom**

a

##### **4.2.1.2. Pristupni uređaji**

a

#### **4.2.2. Usporedba sigurnosnih mehanizama i primjena**

a

### **4.3. Sloj podatkovne poveznice**

a

### **4.3.1. Analiza tehnologije protokola**

a

#### **4.3.1.1. WiFi**

a

#### **4.3.1.2. BLE**

a

#### **4.3.1.3. RFID\NFC**

a

#### **4.3.1.4. ZigBee**

a

#### **4.3.1.5. LTE**

a

#### **4.3.1.6. SigFox**

a

#### **4.3.1.7. LoRaWan**

a

### **4.3.2. Usporedba sigurnosnih mehanizama i primjena**

a

## **4.4. Mrežni sloj**

a

#### **4.4.1. Analiza protokola**

Neki protokoli

##### **4.4.1.1. IPv4**

a

##### **4.4.1.2. IPv6**

a

#### **4.4.2. Usporedba sigurnosnih mehanizama i primjena**

a

### **4.5. Transportni sloj**

a

#### **4.5.1. Usporedba primjena protokola**

a

### **4.6. Aplikacijski sloj**

a

#### **4.6.1. Analiza protokola**

a

##### **4.6.1.1. HTTP/S**

a

##### **4.6.1.2. COAP**

a

#### **4.6.1.3. MQTT**

a

#### **4.6.2. Usporedba sigurnosnih mehanizama i primjena**

a

## **5. Sustav za praćenje tjelesne temperature**

### **5.1. Arhitektura sustava**

a

### **5.2. Korišteni razvojni alati i uređaji**

a

### **5.3. Opis rada sustava**

a

### **5.4. Sigurnosna analiza sustava**

a

## **6. Zaključak**

Zaključak.

# LITERATURA

- [1] Uredba (eu) 2016/679 europskog parlamenta i vijeća, 2016. URL <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=HR>.
- [2] Owasp top ten 2017, May 2017. URL <https://owasp.org/www-project-top-ten/2017>.
- [3] Owasp internet of things, 2018. URL <https://owasp.org/www-project-internet-of-things/>.
- [4] Noah Apthorpe, Dillon Reisman, i Nick Feamster. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *arXiv*, May 2017. URL <https://arxiv.org/abs/1705.06805v1>.
- [5] Jaysson Hollingshead. The 7 Biggest Data Breaches of All Time | InfoSec Insights, Sep 2019. URL <https://sectigostore.com/blog/the-7-biggest-data-breaches-of-all-time>. [Online; accessed 31. May 2021].
- [6] Bernard Meyer. After analyzing 15 billion passwords, these are the most common phrases people use | CyberNews, May 2021. URL <https://cybernews.com/best-password-managers/most-common-passwords>.



## POPIS SLIKA

# POPIS TABLICA

3.1. Primjer DNS upita napravljenih od strane uređaja [4] . . . . .	9
---	---

## **Analiza i usporedba sigurnosnih mehanizama u Internetu stvari**

### **Sažetak**

Sažetak na hrvatskom jeziku.

**Ključne riječi:** Ključne riječi, odvojene zarezima.

### **Title**

### **Abstract**

Abstract.

**Keywords:** Keywords.